FORTINET

The CISO Playbook for Cloud Security

5 Strategies to Navigate Your Evolving Job Description

Table of Contents

The Expanding Role of the CISO

The traditional role of the chief information security officer (CISO) has always been to design cybersecurity strategies that protect data and minimize an organization’s risk profile. Should an event occur, the CISO was responsible for incident response procedures to limit exposure, loss, and unnecessary downtime. Ah... the good old days.

Make no mistake: The CISO is still on the hook for all those obligations. But as companies continue to adopt cloud technologies, CISOs face new challenges. Migrating data and securing critical workloads in the cloud is no joke. CISOs still have to fulfill their traditional responsibilities, but the list of to-dos (and skills to learn) seems to grow by the day.

This playbook offers five “big rocks” that will help CISOs build a leadership role that endures through ever-changing job descriptions. These strategic initiatives will lay the foundation for a security organization that fosters trust among departments while building productive cloud architectures that:

- Speed the execution and accuracy of code
- Embrace automation and increase operational efficiency
- Prioritize risk and mitigate threats faster
- Achieve continuous compliance

#1: Build Champions

Cloud security can be extremely challenging. To be successful, CISOs must gain buy-in from executives across several domains, including risk, privacy, compliance, security, development, and technology. Organizations must understand that providing complete cloud protection against modern threats could require deep operational change. But the day-to-day change starts with a shift in mindset.

Change can be scary, but it's essential. This presents an opportunity for the CISO to reassure business leaders that, if implemented correctly, processes won't be disrupted, data and applications will be protected, and a collaborative environment that enables the organization to drive secure innovation at scale will be established.

Benefits Will Bring Buyers to the Table

To gain support, focus on each team's biggest motivators and demonstrate how they can benefit from a secure cloud architecture. Research indicates that CTOs (or CIOs), CEOs, and boards of directors play the biggest roles in influencing annual cybersecurity budgets.[1] As such, we've created a quick cheat sheet to help you convey the value drivers that matter most to these key individuals and others across your organization.

CEO

Drivers

- Business growth and profitability
- Competitive advantage
- Reputation and brand
- Risk management
- Compliance and governance

Focus on the biggest motivators for each team and demonstrate how they can benefit from a secure cloud architecture.

Conversation tip

Explain in non-technical terms how a secure cloud architecture can promote business growth, accelerate the release of new services, and expand an organization's reach into untapped markets and regions. In addition, highlight that in today's competitive landscape, employees have choices. It's essential to create an inclusive culture using modern architecture and tools to attract and retain top talent, which in turn helps drive innovation and revenue.

CFO/Compliance

Drivers

- Financial performance
- Risk management
- Return on investment
- Operational efficiency
- Business strategy

Conversation tip

Emphasize the cost savings achieved through efficient cloud security tooling versus relying on more traditional tools that require excessive headcount and resources to manage and maintain. In addition, regulatory concerns are top of mind for CFOs and risk and compliance officers. However, keeping up with diverse regulatory requirements and audit requests can be overwhelming. Demonstrate how cloud compliance monitoring across multiple environments can ensure builds and running cloud services meet compliance requirements and that this starts during development.

CTO

Drivers

- Technological innovation
- Scalability
- Security
- Reliability
- Cost optimization

Conversation tip

Highlight the opportunities for IT to have access to stronger data to make better-informed decisions and drive better business outcomes. IT can partner with security to drive secure innovation for cost-effective, functional products and services that generate additional revenue streams. By using the cloud securely, CTOs can cut costs and help development teams build more quickly. This teamwork provides a competitive advantage for the business and helps create a culture of collaboration.

Head of Development

Drivers

- Collaboration and communication
- Scalability and performance
- Streamlining security and development

Conversation tip

Center your conversation on how innovation, paired with security, is critical to the success of the business. Development teams need an architecture that enables them to focus on building code rather than constantly tweaking or fixing it to be secure. In today's market, development teams must be able to move quickly and produce within an environment that scales and integrates security into the build pipeline. Enabling developers to fix security issues during the build process improves productivity and builds relationships between security and developers.

Innovation, paired with security, is critical to the success of the business.

The Board of Directors

Drivers

- Financial performance
- Risk management
- Corporate strategy
- Corporate governance
- Shareholder value

Conversation tip

Without getting into the specifics (yet), start the conversation with how the board plays a critical role in ensuring that the organization is adequately protected. Discuss how this is particularly important in light of new government regulations that are surfacing across the globe. The conversation should focus on how, with the emergence of modern threats, cybersecurity can no longer be an isolated entity within the organization but should impact every part of the company. This holistic approach is necessary to ensure the business delivers the best value for shareholders and stakeholders.

> “We increased our level of confidence with the information coming out of Lacework FortiCNAPP and were able to give management and senior leadership assurance that we had the cloud environment under control.”

– John Turner, Senior Security Architect, LendingTree

#2: Establish Trust with Development

In a fast-paced environment, trust between security and development teams is critical. Unfortunately, developers often perceive security teams as a roadblock to innovation or as fast as a snail. Security teams, not surprisingly, believe that developers go rogue, bypass security, and skip steps that introduce risk. And the research bears this out. According to the Ponemon Institute, 71% of security analysts say developers don't care about the need to secure applications while they're in development, and 53% said that the developers they worked with viewed security as a hindrance to productivity.[2]

However, the truth is that these two teams are critical for each other's success, and CISOs should prioritize efforts to build relationships between them. Again, it begins with a change of mindset. Make conscious efforts to overcome preconceived notions that security can only come at the cost of speed. According to the same Ponemon research, both teams feel increasing pressure to hit their goals, producing applications quickly and maintaining data security. Establish that achieving both of these simultaneously is not only possible but within reach.

Trust between security and development teams begins with a change of mindset.

Trust between these two teams is earned, not given. As such, leaders must create an environment for teams that sets them up for mutual success. CISOs can help by selecting well-integrated tools that foster collaboration and eliminate inefficiencies. By integrating security earlier into the development process, utilizing tools with shared workflows, and prioritizing required fixes based on risk to the business, leaders can align teams and build trust.

Developers won't waste time patching code in irrelevant vulnerabilities, and security will be able to reduce the volume of alerts that bog them down. Together, they can prioritize work, reduce noise, and get products to market securely and efficiently.

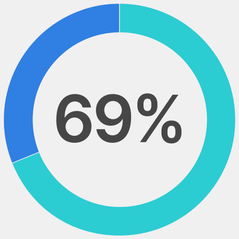
> **"Our DevOps engineers saw Lacework FortiCNAPP in action and fell in love. They couldn't believe it was so simple."**
>
> – David Ramsay, COO, DECTA

#3: Empower Developers to Secure Their Applications

This point is closely related to the prior “big rock” but is nevertheless important enough to stand on its own. Once developer trust is earned and nurtured, begin empowering those developers by seamlessly incorporating security into their processes. This will reduce the time and cost of fixing issues once in a production environment and partially solve your lean security team’s bandwidth issues.

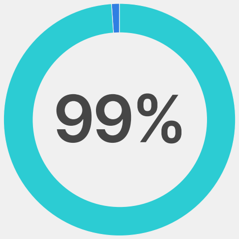
Recently, the adoption of Infrastructure-as-Code (IaC) has reached critical mass. Some research by the Enterprise Strategy Group (ESG) found that more than two-thirds of organizations currently utilize IaC templates and the momentum will only continue to grow.[3] But, too often, cloud architects focus entirely on performance, forgetting about exposure to risks and threats until it’s too late. The same ESG research indicated that, while IaC adoption is increasing, so are the misconfigurations. In fact, 83% of respondents indicated that they’ve experienced an uptick in IaC misconfigurations.

This approach is never as effective as integrating security into the cloud platform from the start. With a solid cloud security architecture, businesses can confidently take advantage of the cloud’s benefits—agility, efficiency, and scale—while mitigating threats and vulnerabilities. CISOs should invest in processes and tooling that allow them to shift left, meaning they integrate security capabilities earlier in the technology process, commonly called DevSecOps. Incorporating security into IaC tooling and continuous integration/continuous delivery (CI/CD) pipelines can automate the integration of code changes from multiple developers into a single codebase and enable developers to enact security without being security experts. It also empowers developers to fix security issues during the build process, preventing delays during production and strengthening the relationship between security and development.



More than two-thirds of organizations currently utilize IaC templates.

You may have hesitations about offloading some security responsibilities to developer teams, but your fears of pushback are largely unfounded. In ESG's research, 99% of surveyed developers indicated some degree of comfort with increased security involvement, with 83% indicating that they were either mostly or completely comfortable. With limited staff and resources, investing in security controls reduces resource burdens, increases operational efficiency, and helps resolve issues during development, not production.



In ESG's research, 99% of surveyed developers indicated some degree of comfort with increased security involvement.

#4: Invest in Data and Automation

Your cloud environment is full of data—data that's tied to your business, your business applications, your cloud infrastructure, and any security signals. The list goes on and on. That's a lot of data to ingest, analyze, secure, and act upon. Yet, many cloud security efficiencies rest on taking all the cloud data within your environment, finding meaningful connections, and acting upon those insights. But that, of course, takes time that security teams simply do not have.

With automation, CISOs have the opportunity to keep up with this growing data set and align the cost of tools and people with measurable security outcomes.

Understanding your cloud data and acting upon it quickly is essential to reduce risks and make smarter decisions that grow the business. Modern security tools can employ automation to help you understand your cloud data; however, analysts have agreed that the best approach to use your data most effectively is through a single security platform.[4] While multiple security solutions may help make sense of your data individually, only a platform approach that accomplishes these functions in aggregate can consider all of your security data and draw correlations between these data points in one place.

Within a single platform, automated data analysis can enable more efficient ways to accomplish traditional use cases. For example, composite alert analysis allows organizations to identify compromises in cloud entities for early and automatic detection of an active attack. Automation that uses behavioral and anomaly detection can quickly spot patterns to surface, analyze, and prioritize the risk to your business so you never miss a critical alert.

Automation can be a lifesaver for understaffed security teams. The icing on the cake is the ability to centrally manage that data with development and operations teams to improve collaboration and speed mitigation within a single platform.

Automation improves productivity, security efficacy, and teamwork between security and development.

#5: Automate Compliance as Much as Possible

In the hit novel The Phoenix Project, the authors discuss the four types of IT work. The fourth type, the dreaded "unplanned work," consists of incidents or requests generated by others, which almost always prevents you from achieving your goals. Unfortunately, for security professionals, unplanned work is all too familiar.

According to the authors, the key to managing unplanned work is to avoid it whenever possible. While some unplanned security work cannot be avoided, it can be automated.

> **"With the reports generated by Lacework FortiCNAPP, we can easily see what resources are compliant, what resources are not compliant, and what we need to do to achieve compliance."**

Enter compliance. Compliance is like laundry; it's never going away. In fact, regulations seem to be increasing in size and scope globally while teams and budgets are shrinking or stagnating. Audit requests will continue, distracting your lean team from strategic, high-value work. This friction presents an opportunity for CISOs to streamline workflows, automate tedious processes, and achieve compliance faster. As a result, CISOs can help their organizations gain a competitive advantage by employing automation to open doors to revenue streams in new regions and markets.

CISOs should look for tools that continuously monitor their environments, automate evidence gathering, and streamline reporting to keep up with the constant requests from clients, partners, auditors, and regulators. This automation can cut costs and reduce errors often associated with manual approaches. CISOs can simplify assessing posture and measuring compliance with PCI, HIPAA, NIST, ISO 27001, and SOC 2 policies. By choosing tools that integrate with existing workflows, CISOs can enable their teams to spot issues quickly and be confident they are protecting their company from liability, fines, and additional costs.

Conclusion

CISOs have the tools to strengthen their influence, create teamwork, and dispel the perception of security as a cost center. The key to success is to build bridges among all stakeholders and design a secure cloud architecture that enables growth, speeds innovation, and ensures compliance with regulations.

Fortinet's Lacework FortiCNAPP platform provides a solution for security teams, developers, operations, and executives to collaborate in proactively securing cloud environments at scale. Our platform enables teams to discover and fix misconfigurations and vulnerabilities, meet compliance, and identify any malicious activity with continuous visibility from build to runtime.

Access more resources and move from playbook to playmaker.
Get started at fortinet.com/cloud.

[1] NewtonX Current, Cybersecurity in 2022: Business Outlook and Key Trends, September, 2021.

[2] Ponemon Institute, The Need to Close the Cultural Divide between Application Security and Developers, September, 2020.

[3] Enterprise Strategy Group, Walking the Line: GitOps and Shift Left Security, August, 2022.

[4] Gartner, Gartner Market Guide for Cloud-Native Application Protection Platforms (CNAPP), April 24, 2023.

FORTINET

www.fortinet.com